Eric A. Grover, Esq. (SBN 136080)
KELLER GROVER LLP
1965 Market Street
San Francisco, California 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861
Email: eagrover@kellergrover.com

Mark S. Reich (*pro hac vice* to be filed)
Courtney E. Maccarone (*pro hac vice* to be filed)
LEVI & KORSINSKY, LLP
55 Broadway, 10th Floor
New York, New York 10006
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com

Counsel for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CARL ALENIUS, individually and on behalf of all others similarly situated, Plaintiff, v. SEQUOIA BENEFITS AND INSURANCE SERVICES, LLC and SEQUOIA ONE PEO, LLC, Defendants.	**Case No.** **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Carl Alenius ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this class action complaint against Defendants Sequoia Benefits and Insurance Services, LLC and Sequoia One PEO, LLC ("Sequoia" or "Defendants"). Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff brings this class action lawsuit on behalf of all persons who entrusted Sequoia with sensitive personal information that was subsequently exposed in a data breach, which Sequoia publicly disclosed on December 7, 2022 (the "Data Breach" or the "Breach").[1]

2. Plaintiff's claims arise from Sequoia's failure to safeguard personally identifying information ("PII") that was entrusted to it in its capacity as a human resources and benefits management company, and its accompanying responsibility to store and transfer that information. Between September 22 and October 6 of 2022, hackers accessed Sequoia's cloud storage system including to its customers' sensitive personal information

3. Sequoia offers customers a method for integrating data, along with employee compensation, and employee benefits management and administrative services. Sequoia One PEO provides services for employee onboarding, risk and safety management, and worker training and development. Sequoia is used by a range of businesses, from startups to public companies. Sequoia has more than 1,700 corporate clients.

4. Sequoia stores sensitive personal data of millions of employees and their family members.

5. Despite acting, and marketing itself, as a safe container for sensitive information, Sequoia failed to take precautions designed to keep that information secure.

6. Sequoia, on or about December 7, 2022, acknowledged that between September 22, 2022, and October 6, 2022, hackers accessed its cloud system that Sequoia uses to store sensitive personal information for its customers' employees and their family members. The data maintained includes names, addresses, dates of birth, employment status, and, significantly, Social Security numbers.

7. Sequoia admits that information in its cloud storage system was accessed by unauthorized individuals. The Data Breach affected millions of consumers in the United States,

[1] *Submitted Breach Notification Sample*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, OFFICE OF THE ATTORNEY GENERAL, https://oag.ca.gov/ecrime/databreach/reports/sb24-559929 (last visited January 5, 2023).

compromising the personal data of individual employees of Defendants' more than 1,700 corporate clients.

8. The sensitive nature of the data exposed through the Data Breach, including Social Security numbers, signifies that Plaintiff and Class members have suffered irreparable harm. They are subject to an increased risk of identity theft.

9. Defendants owe a duty to Plaintiff and Class members to maintain adequate security measures to safeguard the PII it collected and was entrusted them. Defendants breached its duty by failing to implement and/or maintain adequate security practices.

10. Sequoia also delayed, as long as months, to admit and give notice of the Data Breach. It waited despite knowing that hackers accessed its cloud storage system and that sensitive PII was compromised.

11. As a result of the Data Breach, Plaintiff's and Class members' PII has been exposed to criminals for misuse. Plaintiff and the Class have suffered and will continue to suffer injuries, as a result of the Data Breach and the accompanying delay in its disclosure, including: financial losses caused by misuse of PII; the loss or diminished value of their PII as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal, medical, and financial information.

12. Plaintiff brings this action individually and on behalf of a Nationwide Class and New York Subclass of similarly situated individuals against Defendants for: negligence, breach of implied contract, violation of New York General Business Law N.Y. Gen. Bus. Law § 349, and unjust enrichment.

JURISDICTION AND VENUE

13. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendants, and there are more than 100 putative Class members.

14. This Court has personal jurisdiction over Defendants because Defendants maintain their principal place of business in this District, are registered to conduct business in California, and have sufficient minimum contacts with California.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

INTRADISTRICT ASSIGNMENT

16. Under Local Rule 3-2(c) and (d), assignment of this action to the San Francisco or Oakland Division is proper because Defendant Sequoia Benefits and Insurance Services, LLC is headquartered in the County of San Mateo and Defendant Sequoia One PEO, LLC is headquartered in the County of San Francisco, and a substantial part of the events or omissions which give rise to the claims alleged herein occurred in those counties.

PARTIES

17. Plaintiff Carl Alenius is a citizen of New York and resides in Brooklyn, New York. In December 2022, he received a data breach notification letter – dated December 7 – from Sequoia informing him that PII concerning him and his spouse was compromised in the Data Breach. The letter is attached hereto as Exhibit A. As a consequence of the Data Breach, Mr. Alenius has been forced to and will continue to invest significant time monitoring his and his family's accounts to detect and reduce the consequences of likely identity fraud. Plaintiff is subject to substantial and imminent risk of future harm.

18. Defendant Sequoia Benefits and Insurance Services, LLC ("Sequoia Benefits") is a California corporation headquartered at 1850 Gateway Drive, Suite 700, San Mateo, CA 94404. It provides services to enable businesses to manage employee experience, employee statistics, compensation, and benefits.

19. Defendant Sequoia One PEO, LLC ("Sequoia One")[2] is a California corporation headquartered at 22 4th Street, 14th Floor, San Francisco, CA 94103. It manages human resources, payroll, and employee benefits for its business customers.

[2] Defendants Sequoia Benefits and Insurance Services, LLC and Sequoia One PEO, LLC are related entities.

FACTUAL BACKGROUND

A. The Data Breach

20. Hackers gained access to the cloud storage system that Sequoia uses to store PII. The cloud storage contained a range of personal information, including names, addresses, dates of birth, employment status, marital status, and license and Social Security numbers.

21. In early December 2022, Sequoia sent data breach notice letters to the individuals whose data, at least according to Sequoia, was compromised in the breach.

22. Sequoia has not disclosed the number of individuals whose data was compromised in the breach.

23. Sequoia's notification letters state that Sequoia conducted a forensic review of the breach and "found no evidence that the unauthorized party misused or distributed data" at this time.[3] This effort to downplay the breadth of, or impact caused by, the Data Breach has the effect of misleading data breach victims into believing they are not subject to any harm.

24. While Sequoia sought to minimize the damage caused by the breach, it cannot and has not denied that there was unauthorized access to the PII of Plaintiff and Class members.

25. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

B. Sequoia's Obligation to Protect PII

26. Sequoia Benefits, as a human resources, payroll, and benefits management company, provides its customers with software that allows them to simplify employee compensation, health benefits, retirement plans, and compliance.

27. Sequoia One provides outsourced human resource services. Sequoia One primarily markets to startups.

28. Sequoia has an annual revenue of over$180 million. The company has more than 1,700 corporate clients.

[3] *Popular HR and Payroll Company Sequoia Discloses a Data Breach*, WIRED, https://www.wired.com/story/sequoia-hr-data-breach/ (last visited January 5, 2023).

29. As part of its marketing, Sequoia highlights its ability to "establish secure processes for uploading health information, storing medical verification documents, and ensuring only the right people have access to this sensitive data."[4] Sequoia further promotes its cyber security and cyber protection capabilities.[5]

C. Sequoia's Failure to Prevent, Identify and Timely Report the Data Breach.

30. Sequoia failed to take adequate measures to protect its computer and cloud storage systems against unauthorized access.

31. Sequoia was not only aware of the importance of protecting the PII that it maintains, as alleged, it flaunted its capability to do so. The PII Sequoia allowed to be exposed in the Data Breach is the type of private information that Sequoia knew or should have known would be the target of cyberattacks.[6]

32. Despite its own knowledge and supposed expertise on the subject of cybersecurity, and notwithstanding the FTC's data security principles and practices,[7] Sequoia failed to disclose that its systems and security practices were inadequate to reasonably safeguard their sensitive personal information.

---

[4] *Workplace Management*, SEQUOIA, https://www.sequoia.com/platform/workplace/ (last visited on January 5, 2023).

[5] Maria Small, *Cyber Liability in the Time of Covid: Ransomware*, FOREWORD: THE SEQUOIA BLOG (Nov. 2, 2020) https://www.sequoia.com/2020/11/cyber-liability-in-the-time-of-covid-ransomware/ (last visited on January 5, 2023); Jen Scales. *Guide to Cyber Protection*, FOREWORD: THE SEQUOIA BLOG (AUG. 11, 2017) https://www.sequoia.com/2017/08/guide-cyber-protection/ (last visited on January 23, 2023).

[6] Mary Beth Downs, *Biometric Data Collection – State and Federal Legislative Recap*, FOREWORD: THE SEQUOIA BLOG (Aug. 19, 2020), https://www.sequoia.com/2020/08/biometric-data-collection-state-and-federal-legislative-recap/ (last visited January 5, 2023); Sequoia Trust Center, *available at* https://www.sequoia.com/trust/#security (last visited January 5, 2023); Mary Beth Downs, *Cyber Liability Insurance – 10 Tips to Consider*, FOREWORD: THE SEQUOIA BLOG (Jul. 27, 2020), https://www.sequoia.com/2020/07/cyber-liability-insurance-10-tips-to-consider/ (last visited January 5, 2023); Mary Beth Downs, *2020 Cyber Risk Landscape – Let's Do A Deep Dive*, FOREWORD: THE SEQUOIA BLOG (Jul. 16, 2020), https://www.sequoia.com/2020/07/2020-cyber-risk-landscape-letsdo-a-deep-dive/ (last visited January 5, 2023).

[7] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited January 5, 2023).

33. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach.[8] Immediate notification of a Data Breach is critical so that those impacted can take measures to protects themselves. Despite this guidance, Sequoia delayed the notification of the Data Breach.

D. The Harm Caused by the Data Breach Harmed, Now and Going Forward.

34. Victims of data breaches are susceptible to becoming victims of identity theft.

35. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[9]

36. The type of data that was accessed and compromised here – such as, full name, Social Security number – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

37. Plaintiff and class members face a substantial risk of identity theft given that their Social Security numbers, addresses, and dates of birth were compromised. Once a Social Security number is stolen, it can used to identify victims and target them in fraudulent schemes and identity theft.

38. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

[8] *Id.*

[9] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited January 5, 2023).

39. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[10]

40. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[11]

41. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

42. A compromised or stolen Social Security number cannot be addressed as simply as, perhaps, a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security

---

[10] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited January 5, 2023).

[11] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR, April 3, 2018, *available at:* https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited January 5, 2023).

[12] *Id.*

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited January 5, 2023).

number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

43. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[15]

44. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[16]

45. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[17] Defendant did not rapidly report to Plaintiffs and Class members that their PII had been stolen. Sequoia, however, delayed notification of the compromise.

46. Sequoia offered victims three years of free identity protection services. The identity protection services offered by Sequoia is inadequate. Identity thieves often hold onto personal information in order to commit fraud years after such free programs expire.

47. As a result of the Data Breach, the PII of Plaintiffs and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include:

a. unauthorized use of their PII;

---

[14]Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited January 5, 2023).

[15] *Experts advise compliance not same as security*, RELIAS MEDIA https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (Last visited January 5, 2023).

[16]*2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (Last visited January 5, 2023).

[17] *Id.*

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PHI;

e. Improper disclosure of their PII;

f. loss of privacy, and embarrassment;

g. trespass and damage their personal property, including PII/PHI;

h. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

j. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market; and

k. damages to and diminution in value of their PII entrusted to Defendant for the sole purpose of obtaining medical services from Defendant; and the loss of Plaintiffs' and Class members' privacy.

48. In addition to a remedy for economic harm, Plaintiff and Class members maintain an interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

49. Defendant disregarded the rights of Plaintiff and Class members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable

measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

50. The actual and adverse effects to Plaintiff and Class members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

51. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the data breach publicly announced by Sequoia in December 2022 (the "Class").

52. Plaintiff also seeks certification of a New York Subclass, defined as follows:

> All New York residents whose personal information was compromised in the data breach publicly announced by Sequoia in December 2022 (the "New York Subclass").

53. Specifically excluded from the Class are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendants**,** and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendants and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

54. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

55. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

56. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendants, Plaintiff estimates that the Class is comprised of thousands of Class members. The Class is sufficiently numerous to warrant certification.

57. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class Members because they all had their PII compromised as a result of the Data Breach. Plaintiff is a member of the Class and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class members that was caused by the same misconduct by Defendants.

58. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

59. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered

by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendants will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

60. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

a. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendants' storage of Class Member's PII was done in a negligent manner;

d. Whether Defendants had a duty to protect and safeguard Plaintiff's and Class Members' PII?

e. Whether Defendants' conduct was negligent;

f. Whether Defendants' conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendants took sufficient steps to secure their customers' PII;

h. Whether Defendants were unjustly enriched;

i. The nature of relief, including damages and equitable relief, to which Plaintiff and members of the Class are entitled.

61. Information concerning Defendants' policies is available from Defendants' records.

62. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

63. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendants. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

64. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

65. Given that Defendants have not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

66. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

67. Plaintiff brings this claim individually and on behalf of the Class members.

68. Defendants knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

69. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

70. Defendants had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII within its possession was compromised and precisely the type(s) of information that were compromised.

71. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its

systems and networks, and the personnel responsible for them, adequately protected its customers' PII.

72. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their customers. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

73. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

74. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII.

75. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

76. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

77. Failing to adequately monitor the security of its networks and systems;

78. Failure to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

79. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

80. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

81. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the PII within Defendants' possession might have been compromised and precisely the type of information compromised.

82. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff and Class Members' PII would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

83. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in injuries to Plaintiff and Class Members.

84. Defendants' breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

85. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

86. As a result of Defendants' failure to timely notify Plaintiff and Class Members that their PII had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

87. As a result of Defendants' negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

88. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

89. Plaintiff and the Class provided and entrusted their PII to Defendants. Plaintiff and the Class provided their PII to Defendants, either directly or indirectly through Defendants' clients, as part of Defendants' regular business practices.

90. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendants. Implied in these exchanges was a promise by Defendants to ensure that the PII of Plaintiff and Class members in its possession was secure.

91. Pursuant to these implied contracts, Plaintiff and Class members provided Defendants with their PII in order for Defendants to provide their services, for which Defendants are compensated. In exchange, Defendants agreed to, among other things, and Plaintiff understood that Defendants would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members PII in compliance with federal and state laws and regulations and industry standards.

92. Implied in these exchanges was a promise by Defendants to ensure the PII of Plaintiff and Class members in its possession was only used to provide the agreed-upon reasons, and that Defendants would take adequate measures to protect Plaintiff's and Class members' PII.

93. A material term of this contract is a covenant by Defendants that they would take reasonable efforts to safeguard that information. Defendants breached this covenant by allowing Plaintiff's and Class members' PII to be accessed in the Data Breach.

94. Indeed, implicit in the agreement between Defendants and its customers was the obligation that both parties would maintain information confidentially and securely.

95. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class members would provide their PII in exchange for services by Defendants. These agreements were made by Plaintiff and Class members as Defendants' customers.

96. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class members would not have disclosed their PII to Defendants but for the prospect of utilizing Defendants' services. Conversely, Defendants presumably would not have taken Plaintiff's and Class members' PII if it did not intend to provide Plaintiff and Class members with its services.

97. Defendants were therefore required to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure and/or use.

98. Plaintiff and Class members accepted Defendants' offer of services and fully performed their obligations under the implied contract with Defendants by providing their PII, directly or indirectly, to Defendants, among other obligations.

99. Plaintiff and Class members would not have entrusted their PII to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their PII.

100. Defendants breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII.

101. Defendants' failure to implement adequate measures to protect the PII of Plaintiff and Class members violated the purpose of the agreement between the parties.

102. Instead of spending adequate financial resources to safeguard Plaintiff's and Class members' PII, which Plaintiff and Class members were required to provide to Defendants, Defendants instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class members.

103. As a proximate and direct result of Defendants' breaches of its implied contracts with Plaintiff and Class members, Plaintiff and the Class members suffered damages as described in detail above.

COUNT III
VIOLATION OF NEW YORK GENERAL BUSINESS LAW
N.Y. GEN. BUS. LAW § 349
(On behalf of Plaintiff and the New York Subclass)

104. Plaintiff Alenius incorporates by reference all previous allegations as though fully set forth herein.

105. New York Gen. Bus. Law § 349(a) states: "Deceptive acts or practices in the conduct of any business, trade or commerce in the furnishing of any service in this state are hereby declared unlawful."

106. By the acts and conduct alleged herein, Defendants committed unfair or deceptive acts and practices by: a) failing to maintain adequate computer systems and data security practices to safeguard PII; b) failing to disclose that their computer systems and data security practices were inadequate to safeguard PII from theft; and c) continued gathering and storage of PII and other personal information after Defendants knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach.

107. The foregoing deceptive acts and practices were directed at consumers.

108. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to the safety and security of PII.

109. Defendants' acts, practices, and omissions were done in the course of Defendants' business of providing services to consumers in the State of New York.

110. As a direct and proximate result of Defendants' violations of GBL §349, Plaintiff and the Class Members suffered damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

111. Also, as a direct result of Defendants' violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief because Defendants continue to retain their PII and may subject that PII to further data breaches unless injunctive relief is granted., including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring procedures and (ii) submit to future annual audits of those systems and monitoring procedures.

112. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed decisions and to protect Plaintiff, Class Members, and the public from Defendants' unfair, deceptive, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

113. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data security incident was high.

114. Plaintiff and Class Members were injured because: a) they would not have utilized Defendants' services had they known the true nature and character of Defendants' data security practices; b) Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of promises that Defendants would keep their information reasonably secure, and c) Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

115. Plaintiff Alenius and the New York Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and All Class Members)

116. Plaintiff incorporates the above allegations as if fully set forth herein.

117. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

118. Plaintiff conferred a benefit upon Defendants by using Defendant's services.

119. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff. Defendants also benefited from the receipt of Plaintiff's PII, as this was used for Defendants administer its services to Plaintiff and the Class.

120. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's services and his PII because Defendants failed to adequately protect his PII. Plaintiff and the proposed Class would not have provided their PII to Defendants or utilized their services had they known Defendants would not adequately protect their PII.

121. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendants, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring the Defendants' conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury of all issues so triable.

Dated: January 6, 2023

KELLER GROVER, LLP

By: 

Eric A. Grover
1965 Market Street
San Francisco, California 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861
Email: eagrover@kellergrover.com

Mark S. Reich*
Courtney E. Maccarone*
LEVI & KORSINSKY, LLP
55 Broadway, 10th Floor
New York, NY 10006
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com

Counsel for Plaintiff

**pro hac vice* to be filed

EXHIBIT A

Return Mail Processing
PO Box 999
Suwanee, GA 30024

December 7, 2022

324 1 75737 **********AUTO**5-DIGIT 11217
CARL ALENIUS
[redacted]

Re: Notice of Data Breach

Dear Carl Alenius, [redacted]

Sequoia Benefits and Insurance Services LLC ("Company") recently became aware that an unauthorized party may have accessed a cloud storage system that contained personal information provided in connection with the Company's services to its clients, including your employer or, if you are a dependent, your family member's employer.

What Happened? As soon as the Company became aware of the situation, a response plan was initiated and a number of immediate actions were completed, including working with outside counsel to initiate a forensic review by Dell Secureworks, a leading global security firm. That forensic review is now complete, which resulted in the following findings:

- No placement of malicious tools or other software such as ransomware was found.
- No evidence of any threat to client or Company networks was found.
- No evidence of compromise of Company endpoints was found.
- No evidence of data being used or distributed has been found to date.
- No evidence of continuing unauthorized activity in Company systems was found.
- Unauthorized access of information in a cloud storage system occurred between September 22 and October 6, 2022.
- The access was "read only," and there is no evidence that the unauthorized party changed any client data.

Further, based on internal investigation, there have been no instances of service interruption for any client or individuals from this situation. Even though the forensic review found no evidence that the unauthorized party misused or distributed data, the Company is notifying clients and individuals and offering three years of identity protection services through Experian to impacted individuals.

How did Company Respond?
As soon as the Company became aware that an unauthorized party may have accessed a cloud storage system, the Company initiated a response plan and completed a number of actions, including, retaining outside counsel to assist in investigating this matter, activating through counsel Dell Secureworks to conduct a thorough forensic review, and engaging through counsel a separate global consulting firm with cybersecurity expertise to serve as technical advisors to counsel to supplement the security review.

What Information Was Potentially Involved? The unauthorized party may have been able to access some personal information, including demographic information such as name, address, date of birth, gender, marital status, and employment status, social security number, work email address, member ID, wage data for benefits, attachments that

may have been provided for advocate services (if any), and ID cards and any COVID test results or vaccine card that may have been uploaded.

Description of Experian Services:
As mentioned above, there was no evidence of unauthorized use or distribution of personal information; however, the Company is offering complimentary access to Experian IdentityWorks℠ for 36 months.

If you believe there was fraudulent use of your or your dependent's information as a result of this situation and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. Please note that Identity Restoration is available to you and your dependents for 36 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you and your dependents, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 36-month membership. This product provides you and your dependents with superior identity detection and resolution of identity theft. To start monitoring personal information, please follow the steps below:

- Ensure that you **enroll by March 7, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/plus
- Provide this **activation code**: WKB635QSB
- If asked, please provide engagement # **B081408.**

If you are enrolling your minor dependent(s), to whom this letter also is addressed, please follow the steps below:

- Ensure that you **enroll your dependent(s) by March 7, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/minorplus
- Provide this **activation code for each dependent being enrolled**: XEBT83ABP
- If asked, please provide the minor dependent engagement # **B081409.**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this matter or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 844-850-0017 by **March 7, 2023**. Be prepared to provide the applicable engagement number above as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 36-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For your minor dependent enrollees, the IdentityWorks service includes the following features:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do.
To further protect your information, you can take steps to monitor your accounts, obtain your credit reports, or place a fraud alert or security freeze on your credit account. For information on each of these steps, please review **Attachment A**. Depending on your jurisdiction, you may also have additional rights available to you, which you can review in **Attachment B**.

For More Information.
If you have further questions or concerns, or would like an alternative to enrolling online, please call 844-850-0017 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number and/or your minor dependent's engagement number as listed above.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment A: Additional Information on Protecting Your Information

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®	**Experian**	**TransUnion®**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/ credit-report-services	www.experian.com/ freeze/center.html	www.transunion.com/ credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Attachment B: Additional State Law Information

For residents of the *District of Columbia, Iowa, Maryland, North Carolina, Oregon, and Rhode Island*

You may contact your Attorney General for additional information about avoiding identity theft. If you are a Rhode Island resident, you may also file a police report by contacting local or state law enforcement agencies. You may use the following information to contact your attorney general:

Office of the Attorney General
Office of Consumer Protection
400 6th Street NW
Washington, DC 20001
(202) 442-9828
www.oag.dc.gov

Office of the
Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5926 / (888) 777-4590
www.iowaattorneygeneral.gov

Maryland Office of
the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(410) 528-8662
www.marylandattorneygeneral.gov

North Carolina
Department of Justice
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6000
www.ncdoj.gov

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392
www.doj.state.or.us

Rhode Island Office of
the Attorney General
Consumer Protection Division
150 South Main Street
Providence, RI 02903
1 (401) 274-4400
www.riag.ri.gov

For residents of *Massachusetts*:

Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico:*

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.ftc.gov.

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/credit-report-services	www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft